#2

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Takeo OHISHI

Serial No. 09/836,325 : Art Unit: 2131

Filed: April 18, 2001 : Examiner:

For: AUTHENTICATION SYSTEM, AND CONTENTS-INFORMATION SENDER AND RECEIVER : Atty Docket: 0102/0162

SUBMISSION OF PRIORITY DOCUMENTS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Attached hereto please find certified copies of applicant's Japanese applications as follows:

Japanese Patent Application No. 2000-133957 filed May 2, 2000
Japanese Patent Application No. 2000-103743 filed April 2, 2001

Applicant requests the benefit of said May 2, 2000 and April 2, 2001 filing dates for priority purposes pursuant to the provisions of 35 USC 119.

Respectfully submitted,

Louis Woo, RN 31,730
Law Offices of Louis Woo
1901 North Fort Myer Drive, Suite 501
Arlington, VA 22209
(703) 522-8872

Date: May 31 2002

U4-0103-TH(1)

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２０００年 ５月 ２日

出 願 番 号
Application Number: 特願２０００－１３３９５７

出 願 人
Applicant (s): 日本ビクター株式会社

２００１年 ４月１３日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０２８７１９

【書類名】　特許願

【整理番号】　412000346

【あて先】　特許庁長官殿

【国際特許分類】　G06F 19/00

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　大石　剛士

【特許出願人】

【識別番号】　000004329

【氏名又は名称】　日本ビクター株式会社

【代理人】

【識別番号】　100093067

【弁理士】

【氏名又は名称】　二瓶　正敬

【手数料の表示】

【予納台帳番号】　039103

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9004770

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システム

【特許請求の範囲】

【請求項１】　コンテンツ送信側機器とコンテンツ受信側機器とが伝送媒体を介して接続され、前記コンテンツ送信側機器から前記コンテンツ受信側機器にコンテンツを送信するため、前記コンテンツ送信側機器が前記コンテンツ受信側機器の認証を行う第１及び第２のプロセスを有する認証方法であって、

前記第１のプロセスが、

・前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

・前記コンテンツ送信側機器が前記署名が付加された情報を受信するステップと、

・前記コンテンツ送信側機器が前記署名が付加された情報に含まれる前記コンテンツ受信側機器の前記証明情報を認証するステップと、

・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記証明情報を参照して、前記署名を認証するステップと、

・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記識別情報を記録手段に記録するステップとを有し、

前記第１のプロセスに続く前記第２のプロセスにおいて、

・前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

・前記コンテンツ送信側機器が前記第２のプロセスで送信されたコンテンツ受信側機器の前記識別情報を受信するステップと、

・前記コンテンツ送信側機器が前記記録手段に記録された前記コンテンツ受信

側機器の前記識別情報と前記第２のプロセスで前記コンテンツ送信側機器が受信した前記コンテンツ受信側機器の前記識別情報とを照合するステップとを、

有する認証方法。

【請求項２】　前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項１記載の認証方法。

【請求項３】　伝送媒体を介してコンテンツ受信側機器と接続可能であり、前記コンテンツ受信側機器からコンテンツを受信するため、前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器であって、

前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報、又は第２の管理機関により管理されている前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から受信する受信手段と、

前記コンテンツ受信側機器の前記証明情報、又は前記コンテンツ受信側機器の前記証明情報を認証した結果を用いて前記署名を認証する手段と、

前記コンテンツ受信側機器の前記識別情報を記録するための記録手段と、

前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と、前記受信した前記コンテンツ受信側機器の前記識別情報とを照合する照合手段とを、

有するコンテンツ送信側機器。

【請求項４】　前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項３記載のコンテンツ送信側機器。

【請求項５】　伝送媒体を介してコンテンツを送信するコンテンツ送信側機器と接続可能であり、前記コンテンツ送信側機器から前記コンテンツを受信するため、前記コンテンツ送信側機器の認証を受けるコンテンツ受信側機器であって、

前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき

、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とをあらかじめ格納する格納手段と、

前記格納手段にそれぞれ格納されている前記コンテンツ受信側機器の証明情報と前記コンテンツ受信側機器の識別情報とが結合され前記第１の管理機関に付与される署名が付加された情報、又は前記コンテンツ受信側機器の識別情報を前記コンテンツ送信側機器に送信する送信手段を、

有するコンテンツ受信側機器。

【請求項６】　前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項５記載のコンテンツ受信側機器。

【請求項７】　コンテンツ送信側機器からコンテンツを受信するコンテンツ受信側機器と、前記コンテンツ受信側機器にコンテンツを送信するため、第１及び第２のプロセスにより前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器と、前記コンテンツ受信側機器と前記コンテンツ送信側機器とを接続する伝送媒体とを有する認証システムであって、

前記第１のプロセスで、前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で受信された前記コンテンツ受信側機器の前記証明情報が前記コンテンツ送信側機器で認証され、前記コンテンツ受信側機器の前記証明情報が参照されて前記署名が認証され、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ送信側機器の記録手段に記録され、

前記第１のプロセスに続く前記第２のプロセスで、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送

信され、前記コンテンツ送信側機器で、前記コンテンツ送信側機器の前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第２のプロセスで前記コンテンツ送信側機器に受信された前記コンテンツ受信側機器の前記識別情報とが照合される認証システム。

【請求項８】　前記コンテンツ受信側機器の前記証明情報が前記コンテンツ受信側機器の信頼度情報を有することを特徴とする請求項７記載の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル映像信号又はデジタル音声信号からなるコンテンツを、コンテンツ送信側機器からコンテンツ受信側機器に送信するため、コンテンツ送信側機器がコンテンツ受信側機器の認証を行う認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムであって、特に、デジタルインターフェイスを介してデバイス間で伝送する際に、データの改変や複製が行われる可能性のある機器への伝送を排除するために好適な技術に関する。

【０００２】

【従来の技術】

ＩＥＥＥ１３９４などのデジタルインターフェイスが実用化されており、従来、このデジタルインターフェイスを用いてコンテンツを伝送する場合、コンテンツを不正に盗取されて著作権が侵害されるのを防ぐために、暗号化を含むコンテンツ保護プロセスが行われている。このプロセスでは、コンテンツ受信側機器のＩＤがコンテンツ送信側機器に送られ、このＩＤの確認を行いながら伝送が行われる。ところが、これだけではいったんコンテンツ受信側機器にコンテンツが取り込まれてしまうと、コンテンツ受信後のコンテンツの管理はコンテンツ受信側機器に任されてしまうため、コンテンツ受信側機器においてコンテンツの改変や複製を自由に行い得る機器であった場合には、著作権の侵害が容易に行われてしまうという問題があった。

【０００３】

これに対して、本発明者らは、特願平２０００－７９１１２号、特願平２０００－０５７７８５号において、コンテンツ伝送前にコンテンツ受信側機器からコンテンツ送信側機器にコンテンツ受信側機器の信頼度を送信し、その信頼度を評価することによって、コンテンツ送信側機器がコンテンツの伝送を行うか否かを決定できるシステムを提案している。

【０００４】

【発明が解決しようとする課題】

コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信するため、コンテンツ送信側機器がコンテンツ受信側機器の認証を行う際に、例えば認証プロセスがただ１つのみの場合や複数の認証プロセスが独立して存在する場合、認証の途中やコンテンツの送信の途中で、例えば正当なコンテンツ受信側機器（シンクデバイス）が不当なコンテンツ受信側機器（シンクデバイス）に変わったり、接続のための伝送媒体（接続ケーブル）から情報が盗取されたりする場合には、本来送ってはならない不当なコンテンツ受信側機器にコンテンツが送られてしまうことがある。また、例えばコンテンツ送信側機器が正当なコンテンツ受信側機器αの認証を行っても、認証が完了してコンテンツの送信が行われるとき、不正なコンテンツ受信側機器βが正当なコンテンツ受信側機器αのふりをして、コンテンツの受信をしてしまうこともある。

【０００５】

本発明は、コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信する際、コンテンツ送信側機器から所望のコンテンツ受信側機器に、コンテンツを盗取されずに確実に送信可能となるよう認証を行う認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムを提供することを目的とする。

【０００６】

【課題を解決するための手段】

本発明は、上記目的を達成するため、まず第１のプロセスにおいて、コンテンツ受信側機器が第１の管理機関からライセンスを受けている証明となる証明情報と、第２の管理機関により管理されている識別情報とが結合されて署名が付加された情報をコンテンツ送信側機器に送信し、コンテンツ送信側機器が証明情報を

認証し、さらにその証明情報を参照して署名を認証し、識別情報を保存し、続く第２のプロセスにおいて、再びコンテンツ受信側機器が第２の管理機関に管理されている識別情報をコンテンツ送信側機器に送信し、その識別情報をコンテンツ送信側機器で受信して、第１のプロセスで保存された識別情報と照合することにより、コンテンツ送信側機器がコンテンツ受信側機器を認証する。

【０００７】

すなわち、本発明によれば、コンテンツ送信側機器とコンテンツ受信側機器とが伝送媒体を介して接続され、前記コンテンツ送信側機器から前記コンテンツ受信側機器にコンテンツを送信するため、前記コンテンツ送信側機器が前記コンテンツ受信側機器の認証を行う第１及び第２のプロセスを有する認証方法であって、

前記第１のプロセスが

・前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

・前記コンテンツ送信側機器が前記署名が付加された情報を受信するステップと、

・前記コンテンツ送信側機器が前記署名が付加された情報に含まれる前記コンテンツ受信側機器の前記証明情報を認証するステップと、

・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記証明情報を参照して、前記署名を認証するステップと、

・前記コンテンツ送信側機器が前記コンテンツ受信側機器の前記識別情報を記録手段に記録するステップとを有し、

前記第１のプロセスに続く前記第２のプロセスにおいて、

・前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信するステップと、

・前記コンテンツ送信側機器が前記第２のプロセスで送信されたコンテンツ受信側機器の前記識別情報を受信するステップと、

・前記コンテンツ送信側機器が前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第２のプロセスで前記コンテンツ送信側機器が受信した前記コンテンツ受信側機器の前記識別情報とを照合するステップとを、

有する認証方法が提供される。

【０００８】

また、本発明によれば、伝送媒体を介してコンテンツ受信側機器と接続可能であり、前記コンテンツ受信側機器からコンテンツを受信するため、前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器であって、

前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報、又は第２の管理機関により管理されている前記コンテンツ受信側機器の前記識別情報を前記コンテンツ受信側機器から受信する受信手段と、

前記コンテンツ受信側機器の前記証明情報、又は前記コンテンツ受信側機器の前記証明情報を認証した結果を用いて前記署名を認証する手段と、

前記コンテンツ受信側機器の前記識別情報を記録するための記録手段と、

前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と、前記受信した前記コンテンツ受信側機器の前記識別情報とを照合する照合手段とを、

有するコンテンツ送信側機器が提供される。

【０００９】

また、本発明によれば、伝送媒体を介してコンテンツを送信するコンテンツ送信側機器と接続可能であり、前記コンテンツ送信側機器から前記コンテンツを受信するため、前記コンテンツ送信側機器の認証を受けるコンテンツ受信側機器であって、

前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき

、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とをあらかじめ格納する格納手段と、

前記格納手段にそれぞれ格納されている前記コンテンツ受信側機器の証明情報と前記コンテンツ受信側機器の識別情報とが結合され前記第１の管理機関に付与される署名が付加された情報、又は前記コンテンツ受信側機器の識別情報を前記コンテンツ送信側機器に送信する送信手段を、

有するコンテンツ受信側機器が提供される。

【００１０】

また、本発明によれば、コンテンツ送信側機器からコンテンツを受信するコンテンツ受信側機器と、前記コンテンツ受信側機器にコンテンツを送信するため、第１及び第２のプロセスにより前記コンテンツ受信側機器の認証を行うコンテンツ送信側機器と、前記コンテンツ受信側機器と前記コンテンツ送信側機器とを接続する伝送媒体とを有する認証システムであって、

前記第１のプロセスで、前記コンテンツ受信側機器を管理する第１及び第２の管理機関が存在するとき、前記コンテンツ受信側機器の格納手段にそれぞれ格納されたライセンスの存在を示す前記第１の管理機関による証明情報と、前記コンテンツ受信側機器自体を識別する前記第２の管理機関に付与される識別情報とが結合され、この結合情報に前記第１の管理機関に付与される署名が付加された情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で受信された前記コンテンツ受信側機器の前記証明情報が前記コンテンツ送信側機器で認証され、前記コンテンツ受信側機器の前記証明情報が参照されて前記署名が認証され、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ送信側機器の記録手段に記録され、

前記第１のプロセスに続く前記第２のプロセスで、前記コンテンツ受信側機器の前記識別情報が前記コンテンツ受信側機器から前記コンテンツ送信側機器に送信され、前記コンテンツ送信側機器で、前記コンテンツ送信側機器の前記記録手段に記録された前記コンテンツ受信側機器の前記識別情報と前記第２のプロセス

で前記コンテンツ送信側機器に受信された前記コンテンツ受信側機器の前記識別情報とが照合される認証システムが提供される。

【００１１】

また、上記の認証方法、コンテンツ送信側機器、コンテンツ受信側機器、認証システムのそれぞれにおいて、コンテンツ受信側機器の証明情報がコンテンツ受信側機器の信頼度情報を有することは、本発明の好ましい態様である。

【００１２】

【発明の実施の形態】

以下、図面を参照しながら、本発明に係る実施の形態に関して説明する。図１は、本発明に係るソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信するために行われる手順の一実施形態を示すフローチャートである。本発明では、後述する第１のプロセス（ステップＳ１）、第２のプロセス（ステップＳ２）、鍵交換プロセス（ステップＳ３）の認証プロセスを行うことによって、ソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを確実に送信する。

【００１３】

図９は、本発明に係るソースデバイス及びシンクデバイスを構成する手段を示す模式図である。ソースデバイス１とシンクデバイス２とは、ＩＥＥＥ１３９４などのデジタルインターフェイスによって接続されている。ソースデバイス１は、送信手段３、受信手段４、演算手段５、格納手段６、メモリ７、照合手段８を有している。一方、シンクデバイス２は、送信手段３、受信手段４、演算手段５、格納手段６、メモリ７を有している。送信手段３は、接続された機器に対して情報を送信する手段である。受信手段４は、接続された機器から情報を受信する手段である。演算手段５は、あるデータに対して、別のデータを用いて演算を行う手段であり、署名の作成や認証に用いられる。格納手段６は、データを格納しておく手段である。メモリ７は、送受信や演算などを行うときに一時的にデータを記録するための記録手段である。照合手段８は、２つの情報を比較して、それらの情報が一致しているか否かを照合する手段である。また、図示省略している

が、ソースデバイス１及びシンクデバイス２はそれぞれＣＰＵを有しており、このＣＰＵによって各手段の動作が制御されている。

【００１４】

図８は、ソースデバイス及びシンクデバイスが有している格納手段に格納されている情報を示す模式図である。ソースデバイス１の格納手段６には、公開鍵Ｘpub、公開鍵Ｚpub、公開鍵Ｗ２pub、秘密鍵Ｗ２prvが格納されている。一方、シンクデバイス２の格納手段６には、公開鍵Ｙpub（図１２に図示）を含むＡorg証明情報、秘密鍵Ｙprv、第２のプロセス用ＩＤ、公開鍵Ｗ１pub（図１２に図示）を含むＢorg証明情報、秘密鍵Ｗ１prv、公開鍵Ｘpub、公開鍵Ｚpubが格納されている。

【００１５】

第１のプロセスでは、ソースデバイス１の格納手段６に格納されている公開鍵Ｘpubが用いられる。また、シンクデバイス２の格納手段６に格納されている第２のプロセス用ＩＤ、秘密鍵Ｙprv、Ａorg証明情報が用いられる。公開鍵Ｘpubは、第１のプロセスの管理機関Ａorgにライセンスを与えられた全てのデバイスが有する公開鍵である。この公開鍵Ｘpubは、秘密鍵Ｘprvと対になっている。第２のプロセス用ＩＤは、管理機関Ｂorgから与えられた各デバイスに固有の識別子であり、この第２のプロセス用ＩＤによって、各デバイスの識別が可能となる。秘密鍵Ｙprvは、そのデバイスから外部に出されることのない秘密鍵であり、署名signＡ１を作成するのに用いられる。この秘密鍵Ｙprvは、公開鍵Ｙpubと対になっている。

【００１６】

公開鍵Ｙpubは、各デバイスに固有の鍵である秘密鍵Ｙprvを用いて作成された署名を検証するための個々のデバイスに固有の鍵で、管理機関Ａorgにより与えられている。Ａorg証明情報は、あらかじめ管理機関Ａorgにより与えられており、この公開鍵Ｙpubを含む情報に対して、秘密鍵Ｘprvを用いて演算が行われ、署名signＡ１が付加された情報である。このＡorg証明情報として、例えば管理機関Ａorgがライセンシーにのみ与える公開情報を利用することも可能である。なお、秘密鍵Ｘprvは、管理機関Ａorgのみによって管理されるものであり、管理機

関Ａorg以外の第３者が署名signＡ１を含むＡorg証明情報を作成することはできない。

【００１７】

このＡorg証明情報と第２のプロセス用ＩＤとが結合された情報を情報Ａと呼ぶことにする。情報Ａに関しては、Ａorg証明情報と第２のプロセス用ＩＤとに一方向関数を作用させた結果を結合させて、この結合情報を情報Ａとするのが好適である。また、この情報Ａに対して、あらかじめシンクデバイス２が持っている秘密鍵Ｙprvを用いて演算が行われる。この情報Ａは、あらかじめ一括してシンクデバイス２に付与されているのが好適である。また、署名signＡ２が付加された情報を情報Ｂと呼ぶことにする。この情報Ｂが、後述する第１のプロセスにおいて、シンクデバイス２からソースデバイス１に送信される。署名signＡ１の情報を参照することで、秘密鍵Ｘprvを用いて作成された署名signＡ１が付加された公開鍵Ｙ１pubが改ざんされているか否かを判断することが可能となる。また、署名signＡ２の情報を参照することで、秘密鍵Ｙprvを用いて作成された署名signＡ２が付加されている情報Ａが改ざんされているか否かを判断することが可能となる。

【００１８】

第２のプロセス及び鍵交換プロセスでは、ソースデバイス１の格納手段６に格納されている秘密鍵Ｗ２prv、公開鍵Ｚpub、公開鍵Ｗ２pubが用いられる。また、シンクデバイス２の格納手段６に格納されている秘密鍵Ｗ１prv、第２のプロセス用ＩＤ、公開鍵Ｗ１pub（図１２に図示）を含むＢorg証明情報、公開鍵Ｚpubが用いられる。公開鍵Ｚpubは、管理機関Ｂorgにライセンスを与えられた全てのデバイスが有する公開鍵である。この公開鍵Ｚpubは、秘密鍵Ｚprvと対になっている。なお、秘密鍵Ｚprvは、管理機関Ｂorgのみによって管理されるものであり、管理機関Ｂorg以外の第３者が署名signＢ１を含むＢorg証明情報を作成することはできない。

【００１９】

第２のプロセス用ＩＤと公開鍵Ｗ１pubとが結合された情報を情報Ｃと呼び、この情報Ｃに対して秘密鍵Ｚprvを用いて演算が行われ、署名signＢ１が付加さ

れた情報をＢorg証明情報と呼ぶことにする。このＢorg証明情報が、後述する第２のプロセスにおいて、シンクデバイス２からソースデバイス１に送信される。署名signＢ１の情報を参照することで、秘密鍵Ｚprvを用いて作成された署名signＢ１が付加されたＢorg証明情報が改ざんされているか否かを判断することが可能となる。

【００２０】

公開鍵Ｗ１pub、公開鍵Ｗ２pub、秘密鍵Ｗ１prv、秘密鍵Ｗ２prvは鍵交換プロセスで用いられる鍵であり、後述のように、第２のプロセスで公開鍵Ｗ１pubと公開鍵Ｗ２pubがソースデバイス１とシンクデバイス２との間で交換される。公開鍵Ｗ１pub及び公開鍵Ｗ２pubは、管理機関Ｂorgによってライセンスが与えられた全ての機器が有する鍵であり、秘密鍵Ｗ１prv及び秘密鍵Ｗ２prvは、管理機関Ｂorgによって各デバイスに対して与えられた固有の鍵である。

【００２１】

＜第１のプロセス＞

図１は、本発明に係る第１のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。ステップＳ１０１において、受信手段４によりシンクデバイス２から情報Ｂを受信する。受信するまでは待ち状態になっている。図１２（ａ）は、情報Ｂの構成を示す模式図である。情報Ｂはシンクデバイス２の格納手段６に格納されている情報により構成されており、Ａorg証明情報と第２のプロセス用ＩＤとが結合された情報Ａに対して、あらかじめシンクデバイス２が持っている秘密鍵Ｙprvを用いて演算が行われ、署名signＡ２が付加された情報である。

【００２２】

ステップＳ１０３において、ステップＳ１０１で受信した情報Ｂに含まれる公開鍵Ｙpubが改ざんされていないことを確認する。例えば、公開鍵Ｙpubに付加されている署名signＡ１の一部は元々の公開鍵Ｙpubのデータから派生したものであり、ソースデバイス１において、ステップＳ１０１で受信した情報Ｂ内の公開鍵Ｙpubを含む情報に対して、あらかじめソースデバイス１が持っている公開鍵Ｘpubを用いて演算手段５により演算を行い、この演算結果が上記の署名signＡ

１の一部と同一であることを確認することによって、公開鍵Ｙpubが改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図１１に示すステップＳ１９９において、認証は失敗となり処理を終了する。なお、フローチャートに示されている①は、図１１の①に繋がっている。

【００２３】

次に、ステップＳ１０５において、ステップＳ１０１で受信した情報Ｂに含まれる第２のプロセス用ＩＤが改ざんされていないことを確認する。例えば、第２のプロセス用ＩＤを含む情報Ａに付加されている署名signＡ２の一部は元々の情報Ａのデータから派生したものであり、ソースデバイス１において、ステップＳ１０１で受信した情報Ｂ内の情報Ａに対して、ステップＳ１０３で改ざんされていないことを確認したソースデバイス１が持っている公開鍵Ｙpubを用いて演算手段５により演算を行い、この演算結果が上記の署名signＡ２の一部と同一であることを確認することによって、情報Ａ及び情報Ａ内の第２のプロセス用ＩＤが改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図１１に示すステップＳ１９９において、認証は失敗となり処理を終了する。

【００２４】

ステップＳ１０７において、ステップＳ１０１で受信した情報Ｂに含まれる第２のプロセス用ＩＤをメモリ７に記録する。保存された第２のプロセス用ＩＤは、後述の認証プロセス（第２のプロセス）において用いられる。次に、ステップＳ１０９において、ステップＳ１０１で受信した情報Ｂの認証に成功したことを送信手段３によりシンクデバイス２に通知する。以上が第１のプロセスにおけるソースデバイス１のフローチャートである。

【００２５】

次に、シンクデバイス２の動作に関して説明する。図２は、本発明に係る第１のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。ステップＳ２０１において、送信手段３によりソースデバイス１に情報Ｂを送信する。情報Ｂは、Ａorg証明情報と第２のプロセス用ＩＤとが結合された情報Ａに対して、あらかじめシンクデバイス２が持っている秘密鍵Ｙprvを用い

て演算が行われ、署名signＡ２が付加された情報であるが、この署名signＡ２の付加をシンクデバイス内で行うことも可能であり、また、あらかじめ署名signＡ２が付加された情報を格納手段に格納しておくことも可能である。情報Ｂを送信した後は、ステップＳ２０３でソースデバイス１から認証の成功の通知を受信するまで待ち状態となる。以上が第１のプロセスにおけるシンクデバイスのフローチャートである。

【００２６】

また、前述した特願平２０００－７９１１２号、特願平２０００－０５７７８５号に記載されている認証システムを利用して、ソースデバイス１にシンクデバイス２の信頼度情報を送信するときに、ソースデバイス１への信頼度情報の送信とステップＳ２０１での公開鍵Ｙpub、第２のプロセス用ＩＤの送信を同時に行うことも可能である。信頼度情報は所定の管理機関から与えられる情報であり、この信頼度情報を管理する管理機関と第１のプロセスの管理機関Ａorgが同一の場合には、公開鍵Ｙpubと信頼度情報とが結合されて、１つの署名で裏書きしたものをＡorg証明情報とすることも可能である。

【００２７】

この場合、ソースデバイス１では、ステップＳ１０５とステップＳ１０７の間に、シンクデバイス２の信頼度がコンテンツの送信が可能な信頼度か否かを判断するステップが付加されることが好ましい。この場合、コンテンツの伝送を行ってもいいと判断する基準となる信頼度をソースデバイス１が有しており、この基準となる信頼度よりもシンクデバイス２の信頼度のほうが低い場合は、ソースデバイス１からのコンテンツの送信は不可能と判断され、処理を終了する。

【００２８】

また、上記第１のプロセスにおいて、ステップＳ１０９でソースデバイス１からシンクデバイス２に認証の成功を通知する代わりに、ソースデバイス１が持っているＡorg証明情報をシンクデバイス２に送信するステップを付加して、シンクデバイス２においてもソースデバイス１の認証を行うようにすることも可能である。この場合、シンクデバイス２が認証側、ソースデバイス１が被認証側となって、シンクデバイス２でステップＳ１０１からステップＳ１０７の動作が、ソ

ースデバイス１でステップＳ２０１からＳ２０３の動作が行われる。また、この場合、ソースデバイス１も管理機関Ａorgから Ａorg証明情報が与えられており、さらに、秘密鍵Ｙprvを有していて、署名signＡ２の作成が可能である必要がある。これらのステップにより、不当なソースデバイス１が、正当なシンクデバイス２に対して何度も何度も情報提供を要求して暗号解読をしようという操作を途中で停止させることが可能となり、ソースデバイス１及びシンクデバイス２により構成されるシステム全体の破壊に対する強度を強めることが可能となる。

【００２９】

＜第２のプロセス＞

図３は、本発明に係る第２のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。ステップＳ１１１において、シンクデバイス２からＢorg証明情報を受信手段４により受信する。図１２（ｂ）は、Ｂorg証明情報の構成を示す模式図である。Ｂorg証明情報は、第２のプロセス用ＩＤと公開鍵Ｗ１pubとが結合された情報Ｃに署名signＢ１が付加されたものである。前述した情報Ａの場合と同様、第２のプロセス用ＩＤと公開鍵Ｗ１pubとの結合は、単にそれぞれの情報をつなぐだけでもよく、また、これらの情報に一方向関数を作用させた結果を結合させてもよい。シンクデバイス２からＢorg証明情報を受信できず、所定の時間、待ち状態が続いた場合はタイムアウトとなり、図１１に示すステップＳ１９９において、処理を終了する。ステップＳ１１３において、ステップＳ１１１で受信したＢorg証明情報内の情報Ｃ（第２のプロセス用ＩＤ及び公開鍵Ｗ１pub）が改ざんされていないことを確認する。例えば、情報Ｃに付加されている署名signＢ１の一部は元々の情報Ｃから派生したものであり、ソースデバイス１において、ステップＳ１１１で受信したＢorg証明情報内の情報Ｃに対して、あらかじめソースデバイス１が持っている公開鍵Ｚpubを用いて演算手段５により演算を行い、この演算結果が上記の署名signＢ１の一部と同一であることを確認することによって、情報Ｃが改ざんされていないことが証明される。改ざんされていないことが確認できない場合は、図１１に示すステップＳ１９９において、認証は失敗となり処理を終了する。

【００３０】

ステップＳ１１５において、ステップＳ１０７でメモリに保存された第２のプロセス用ＩＤと、ステップＳ１１１で受信したＢorg証明情報に含まれる第２のプロセス用ＩＤとが一致しているか否かを照合手段８により照合する。両者が一致した場合、ソースデバイス１はシンクデバイス２を正常に認証できたとして、コンテンツの伝送の手順が行われる。一方、両者が異なる場合、図１１に示すステップＳ１９９において、認証は失敗となり処理を終了する。ステップＳ１１５で認証が成功した場合、ステップＳ１１６において、送信手段３により公開鍵Ｗ２pubをシンクデバイス２に送信する。このステップＳ１１６での公開鍵Ｗ２pubの送信の際、ステップＳ１１１でシンクデバイス２から受信した情報のように公開鍵Ｗ２pubをソースデバイス１の第２のプロセス用ＩＤと結合して、さらに署名を付加した情報を送信してもよい。以上が第２のプロセスにおけるソースデバイス１のフローチャートである。

【００３１】

一方、第２のプロセスにおけるシンクデバイス２の動作は以下の通りである。図４は、本発明に係る第２のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。ステップＳ２０５において、送信手段３によりＢorg証明情報をソースデバイス１に送信する。Ｂorg証明情報には、第２のプロセス用ＩＤと公開鍵Ｗ１pubが含まれている。次に、ステップＳ２０６において、ステップＳ１１６でソースデバイス１から送信された公開鍵Ｗ２pubを受信手段４により受信する。ソースデバイス１でＢorg証明情報の認証が成功した場合、鍵交換プロセスが行われるまで待ち状態となる。

【００３２】

ステップＳ２０６で受信した公開鍵Ｗ２pubがソースデバイス１の第２のプロセス用ＩＤと結合されて、さらに署名が付加されている情報の場合、ソースデバイス１で行われたステップＳ１１１からＳ１１５までの認証プロセスをシンクデバイス２で行うことも可能である。これにより、ソースデバイス１及びシンクデバイス２のそれぞれにおいて、第２のプロセスによる相手機器の認証が可能となる。以上が第２のプロセスにおけるシンクデバイス２のフローチャートである。このようにして、第２のプロセスにおいて、公開鍵Ｗ１pubと公開鍵Ｗ２pubがソ

ースデバイス１とシンクデバイス２との間で交換される。

【００３３】

＜鍵交換プロセス＞

一方、コンテンツの伝送の際に行われる鍵交換プロセスは以下の通りである。図５は、鍵交換プロセスにおけるソースデバイスの動作を示すフローチャートである。ステップＳ１１７において、ソースデバイス１が持っている所定のデータに対して、あらかじめソースデバイス１が持っている秘密鍵Ｗ２prvを用いて演算手段５により演算を行い、データを生成する。ステップＳ１１９において、送信手段３により生成されたデータをシンクデバイス２に送信する。ステップＳ１２１において、受信手段４によりシンクデバイス２からデータを受信する。このデータは、シンクデバイス２において、後述するステップＳ２１５（図６に記載）で生成されたデータである。ステップＳ１２３において、シンクデバイス２から受信したデータに対して、先の過程でシンクデバイス２から受信した公開鍵Ｗ１pubを用いて演算手段５により演算を行い、この結果、暗号化鍵Ｕが生成される。ステップＳ１２５において、この暗号化鍵Ｕを、シンクデバイス２のメモリ７に保存する。

【００３４】

図６は、鍵交換プロセスにおけるシンクデバイスの動作を示すフローチャートである。ステップ２０７において、ソースデバイス１からデータを受信手段４により受信する。このデータは、ソースデバイス１において、ステップＳ１１９で生成されたデータである。ステップＳ２０９において、ソースデバイス１から受信したデータに対して、ステップＳ２０６でソースデバイス１から受信した公開鍵Ｗ２pubを用いて演算手段５により演算を行い、この結果、暗号化鍵Ｖが生成される。ステップＳ２１１において、この暗号化鍵Ｖをシンクデバイス２のメモリ７に保存する。ステップＳ２１３において、シンクデバイス２が持っている所定のデータに対して、あらかじめシンクデバイス２が持っている秘密鍵Ｗ１prvを用いて演算手段５により演算を行い、データを生成する。ステップＳ２１５において、送信手段３により生成されたデータをソースデバイス１に送信する。

【００３５】

この鍵交換プロセスにより、ソースデバイス１、シンクデバイス２は、それぞれ暗号化鍵Ｕ、暗号化鍵Ｖを有することになる。この暗号化鍵Ｕと暗号化鍵Ｖとは同一のものである。したがって、コンテンツの送信の際に、ソースデバイス１側で暗号化鍵Ｕを用いてコンテンツを暗号化すれば、暗号化されたコンテンツの復号が可能であるシンクデバイス２、すなわち暗号化鍵Ｖを有するシンクデバイス２だけが、受信したコンテンツの復号を行うことができる。このようにして、ソースデバイス１から特定のシンクデバイス２にコンテンツの送信を行うことが可能となる。

【００３６】

また、図１３は、上記第１のプロセス、第２のプロセス、鍵交換プロセスにおけるソースデバイス及びシンクデバイスの動作をまとめて示すタイムチャートである。このタイムチャートは、上記の図１から図６までのフローチャートをまとめたものであり、図の左側はソースデバイス１、図の右側はシンクデバイス２、両者の間を結ぶ線はソースデバイス１とシンクデバイス２との間の情報の伝送を示している。

【００３７】

次に、図１３に示した認証プロセスの全体の流れを参照して、正当なシンクデバイス２になりすまして、不正なシンクデバイス２がコンテンツを受信しようと企てる“なりすまし”の様々な状況を想定して説明する。図７は、コンテンツの伝送の際に考えられる不正なシンクデバイス２を排除する過程を示す模式図である。今、管理機関Ａorgからのライセンスを受けていない不当なシンクデバイス２が、正当なシンクデバイス２になりすまして、コンテンツを受けようとしている場合を考える。ただし不当なシンクデバイス２は管理機関Ｂorgのライセンスは受けているものとする。

【００３８】

不当なシンクデバイス２が、正当なシンクデバイス２が第１のプロセスで送った情報を盗取して、ソースデバイス１から認証を得ようとする場合、

（Ａ１）同じものを送る場合。

第２のプロセス用ＩＤを含むＡorg証明情報は、正当なシンクデバイス２のも

のである。したがって、不当なシンクデバイス２がこの情報を送った場合、ソースデバイス１は、正当なシンクデバイス２から送信されたものと判断して、不当なシンクデバイス２の“なりすまし”は見破られない。

（Ａ２）第２のプロセス用ＩＤを不当なシンクデバイス２のものに変えて送る場合。

秘密鍵Ｙprvが正当なシンクデバイス２と異なるため、署名signＡ２が正当なシンクデバイス２のものと異なってしまい、不当なシンクデバイス２であることが明らかとなる。

【００３９】

上記（Ａ１）の場合、不当なシンクデバイス２は、第１のプロセスで認証される。このように第１のプロセスで認証された不当なシンクデバイス２は、再び第２のプロセスにおいて認証される必要がある。

（Ｂ１）正当なシンクデバイス２のＢorg証明情報を盗取して、同じものを送る場合。

Ｂorg証明情報の第２のプロセス用ＩＤ及び公開鍵Ｗ１pubは正当なシンクデバイス２のものである。したがって、ステップＳ１１５において、ステップＳ１０７で保存した第２のプロセス用ＩＤとステップＳ１１１で受信したＢorg証明情報内の第２のプロセス用ＩＤとの照合を行った場合、両者は一致するので、不当なシンクデバイス２の“なりすまし”は見破られない。

【００４０】

（Ｂ２）不当なシンクデバイス２の第２のプロセス用ＩＤが含まれるようにＢorg証明情報を改ざんして送る場合。

不当なシンクデバイス２も管理機関Ｂorgのライセンスを受けているので、第２のプロセス用ＩＤの認証のみが行われるならば、認証されてしまう。しかし、本発明では、ステップＳ１１５において、前もってステップＳ１０７で保存した第２のプロセス用ＩＤとステップＳ１１１で受信したＢorg証明情報内の第２のプロセス用ＩＤとの照合を行い、両者が一致しないことを確かめるので、不当なシンクデバイス２の“なりすまし”であることが明らかとなる。

【００４１】

（Ｂ１）で認証された不当なシンクデバイス２も次の鍵交換プロセスにおいて、不当なシンクデバイス２であることが明らかとなってしまう。鍵交換プロセスにおいて、ソースデバイス１に送信される秘密鍵Ｗ１prvは不当なシンクデバイス２のものであるため、伝送するコンテンツを暗号化するときの暗号化鍵Ｖは正当なシンクデバイス２の公開鍵Ｗ１pubと不当なシンクデバイス２の秘密鍵Ｗ１prvを用いて作られることになってしまう。したがって、この暗号化鍵Ｖを用いてコンテンツを暗号化してソースデバイス１から送信しても、シンクデバイス２でコンテンツをデコードすることは不可能である。

【００４２】

また、鍵交換プロセスの代わりに、ソースデバイス１からシンクデバイス２にコンテンツを送信しながら、所定の時間間隔ごとに第２のプロセスを行って、ステップＳ１０７でメモリに保存された第２のプロセス用ＩＤと、ステップＳ１１１で受信したＢorg証明情報に含まれる第２のプロセス用ＩＤとが一致しているか否かを比較することも可能である。この方法でも、コンテンツの送信の途中で正当なシンクデバイス２から不当なシンクデバイス２にコンテンツが送信されてしまうことを防ぎ、所望の相手機器にのみコンテンツを送信することが可能となる。

【００４３】

図１０は、ソースデバイスとシンクデバイスの様々な接続形態を示す図である。上記実施形態では、ソースデバイス１とシンクデバイス２との接続形態は、図１０（ａ）に示すようなＩＥＥＥ１３９４による１対１の接続の他に、図１０（ｃ）に示す１対多が可能であり、また、図１０（ｂ）、図１０（ｄ）のようにインターネットなどのネットワークを介しての接続も可能である。

【００４４】

また、コンテンツ送信側において、シンクデバイス２を認証する機能を有する認証装置を、シンクデバイス２にコンテンツの送信を行うコンテンツ送信装置から独立なものとすることが可能である。また、コンテンツ受信側においても同様に、ソースデバイス１に認証される機能を有する被認証装置を、ソースデバイス１からコンテンツを受信するコンテンツ受信装置から独立なものとすることが可

能である。

【００４５】

本発明によれば、［特許請求の範囲］の欄に記載された発明の他に、次のような発明が提供される。

（１）前記証明情報が、前記結合情報に付加される前記署名を認証するために必須な情報の一部を有することを特徴とする請求項１又は２記載の認証方法。

（２）前記証明情報が、前記第１の管理機関に著作権が存在する著作物を有することを特徴とする請求項１又は２記載の認証方法。

（３）前記証明情報と前記識別情報とに対して、一方向関数を作用させて前記結合情報を生成するステップを有することを特徴とする請求項１又は２記載の認証方法。

（４）前記証明情報を認証するステップにおいて、前記第１の管理機関がライセンシーのみを与える公開情報を利用して、前記証明情報を認証することを特徴とする請求項１又は２記載の認証方法。

（５）前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする請求項１又は２記載の認証方法。

（６）前記証明情報が、前記第１の管理機関により一括してコンテンツ受信側機器に付与されていることを特徴とする請求項１又は２記載の認証方法。

（７）前記第２のプロセスに続く認証プロセスとして、前記第２のプロセスで用いられた情報を利用して鍵交換プロセスを行うステップを有することを特徴とする請求項１又は２記載の認証方法。

【００４６】

（８）前記証明情報が、前記結合情報に付加される前記署名を認証するために必須な情報の一部を有することを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（９）前記証明情報が、前記第１の管理機関に著作権が存在する著作物を有することを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（１０）前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数

を作用させて生成されたものであることを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（１１）前記署名を認証する手段において、前記第１の管理機関がライセンシーのみを与える公開情報を利用して、前記証明情報が認証されることを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（１２）前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（１３）前記証明情報が、前記第１の管理機関により一括して付与されていることを特徴とする請求項３又は４記載のコンテンツ送信側機器。

（１４）前記コンテンツ受信側機器から受信した情報を利用して鍵交換プロセスを行うための手段を有することを特徴とする請求項３又は４記載のコンテンツ送信側機器。

【００４７】

（１５）前記証明情報が、前記結合情報に付加される前記署名を認証するために必須な情報の一部を有することを特徴とする請求項５又は６記載のコンテンツ受信側機器。

（１６）前記証明情報が、前記第１の管理機関に著作権が存在する著作物を有することを特徴とする請求項５又は６記載のコンテンツ受信側機器。

（１７）前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数を作用させて生成されたものであることを特徴とする請求項５又は６記載のコンテンツ受信側機器。

（１８）前記証明情報又は前記証明情報に含まれる署名認証のための情報が、各機器に関してそれぞれ異なるものであることを特徴とする請求項５又は６記載のコンテンツ受信側機器。

（１９）前記証明情報が、前記第１の管理機関により一括して付与されていることを特徴とする請求項５又は６記載のコンテンツ受信側機器。

（２０）前記コンテンツ送信側機器から受信した情報を利用して鍵交換プロセスを行うための手段を有することを特徴とする請求項５又は６記載のコンテンツ受

信側機器。

【００４８】

（２１）前記証明情報が、前記結合情報に付加される前記署名を認証するために必須な情報の一部を有することを特徴とする請求項７又は８記載の認証システム。

（２２）前記証明情報が、前記第１の管理機関に著作権が存在する著作物を有することを特徴とする請求項７又は８記載の認証システム。

（２３）前記結合情報が、前記証明情報と前記識別情報とに対して、一方向関数を作用させて生成されたものであることを特徴とする請求項７又は８記載の認証システム。

（２４）前記コンテンツ送信側機器が有する前記署名を認証する手段において、前記第１の管理機関がライセンシーのみを与える公開情報を利用して、前記証明情報が認証されることを特徴とする請求項７又は８記載の認証システム。

（２５）前記証明情報又は前記証明情報に含まれる署名認証のための情報が、前記コンテンツ受信側機器のそれぞれに関して異なるものであることを特徴とする請求項７又は８記載の認証システム。

（２６）前記証明情報が、前記第１の管理機関により一括して前記コンテンツ受信側機器に付与されていることを特徴とする請求項７又は８記載の認証システム。

（２７）前記コンテンツ送信側機器及び前記コンテンツ受信側機器が、前記第２のプロセスで用いられた情報を利用して前記第２のプロセスに続いて鍵交換プロセスを行うための手段を有することを特徴とする請求項７又は８記載の認証システム。

【００４９】

【発明の効果】

本発明によれば、まず第１のプロセスにおいて、コンテンツ受信側機器（シンクデバイス）が第１の管理機関からライセンスを受けている証明となる証明情報と、第２の管理機関により管理されている識別情報とが結合されて、署名が付加された情報をコンテンツ送信側機器（ソースデバイス）に送信し、コンテンツ送

信側機器が証明情報を認証し、さらにその証明情報を参照して署名を認証し、識別情報を保存し、続く第２のプロセスにおいて、再びコンテンツ受信側機器が第２の管理機関に管理されている識別情報をコンテンツ送信側機器に送信し、その識別情報をコンテンツ送信側機器で受信して、第１のプロセスで保存された識別情報と照合することにより、コンテンツ送信側機器がコンテンツ受信側機器を認証するので、第２のプロセス用ＩＤや、管理機関Ａorgからライセンスを受けている証明となる証明書によって守られた（改ざんの検出が可能となっている）信頼度情報と公開鍵（署名signＡ１に守られている）とペアになるべき第２プロセス用ＩＤ（署名signＡ２に守られている）が他者に改ざんされたりするのを防ぐことが可能となり、コンテンツ送信側機器からコンテンツ受信側機器にコンテンツを送信する際、コンテンツ送信側機器から所望のコンテンツ受信側機器にコンテンツを盗取されずに確実に送信可能となる。

【図面の簡単な説明】

【図１】

本発明に係る第１のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。

【図２】

本発明に係る第１のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。

【図３】

本発明に係る第２のプロセスの一実施形態におけるソースデバイスの動作を示すフローチャートである。

【図４】

本発明に係る第２のプロセスの一実施形態におけるシンクデバイスの動作を示すフローチャートである。

【図５】

鍵交換プロセスにおけるソースデバイスの動作を示すフローチャートである。

【図６】

鍵交換プロセスにおけるシンクデバイスの動作を示すフローチャートである。

【図７】

コンテンツの伝送の際に考えられる不正なシンクデバイスを排除する過程を示す模式図である。

【図８】

ソースデバイス及びシンクデバイスが有している格納手段に格納されている情報を示す模式図である。

【図９】

本発明に係るソースデバイス及びシンクデバイスを構成する手段を示す模式図である。

【図１０】

ソースデバイスとシンクデバイスの様々な接続形態を示す図である。

【図１１】

本発明に係るソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信するために行われる手順の一実施形態を示すフローチャートである。

【図１２】

（ａ）は、情報Ｂの構成を示す模式図である。

（ｂ）は、Ｂorg証明情報を示す模式図である。

【図１３】

第１のプロセス、第２のプロセス、鍵交換プロセスにおけるソースデバイス及びシンクデバイスの動作をまとめて示すタイムチャートである。

【符号の説明】

１　ソースデバイス（コンテンツ送信側機器）

２　シンクデバイス（コンテンツ受信側機器）

３　送信手段

４　受信手段

５　演算手段

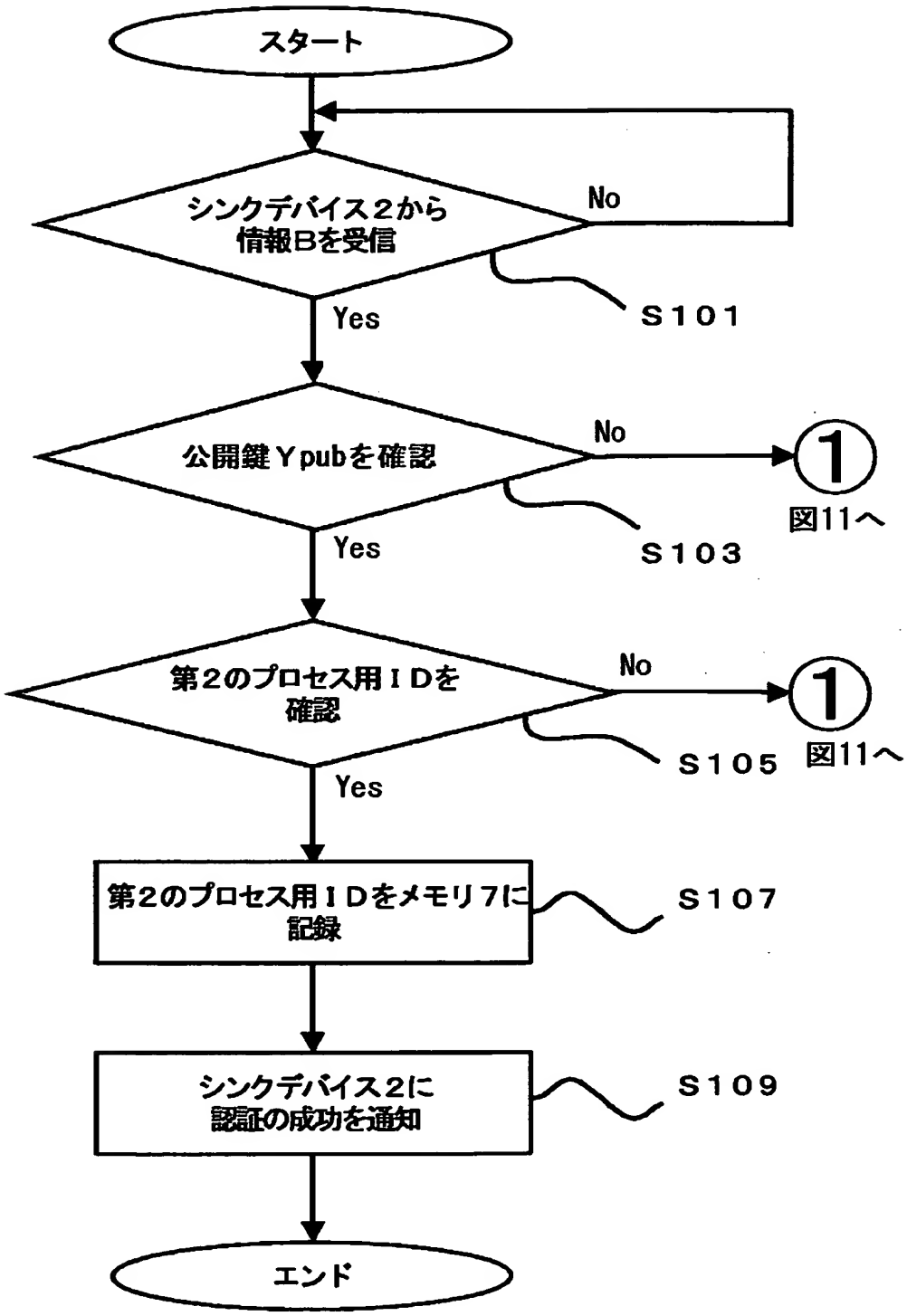
６　格納手段

７　メモリ

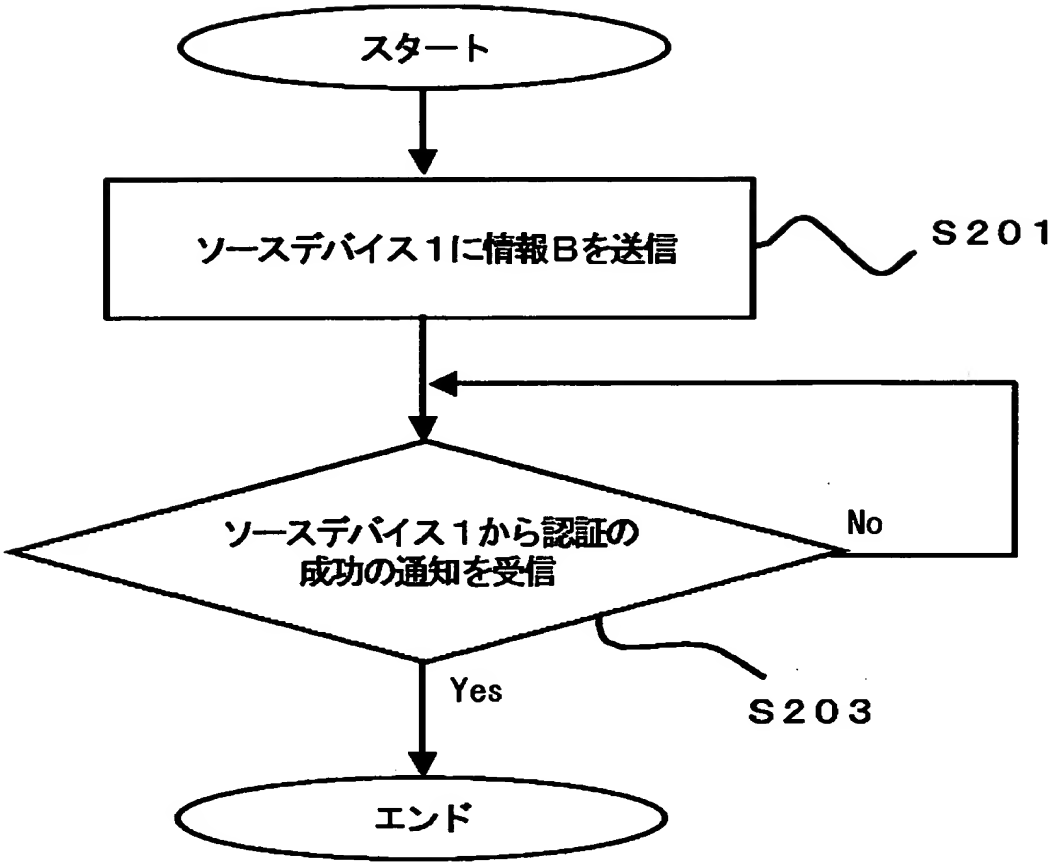
８　照合手段

【書類名】　　図面

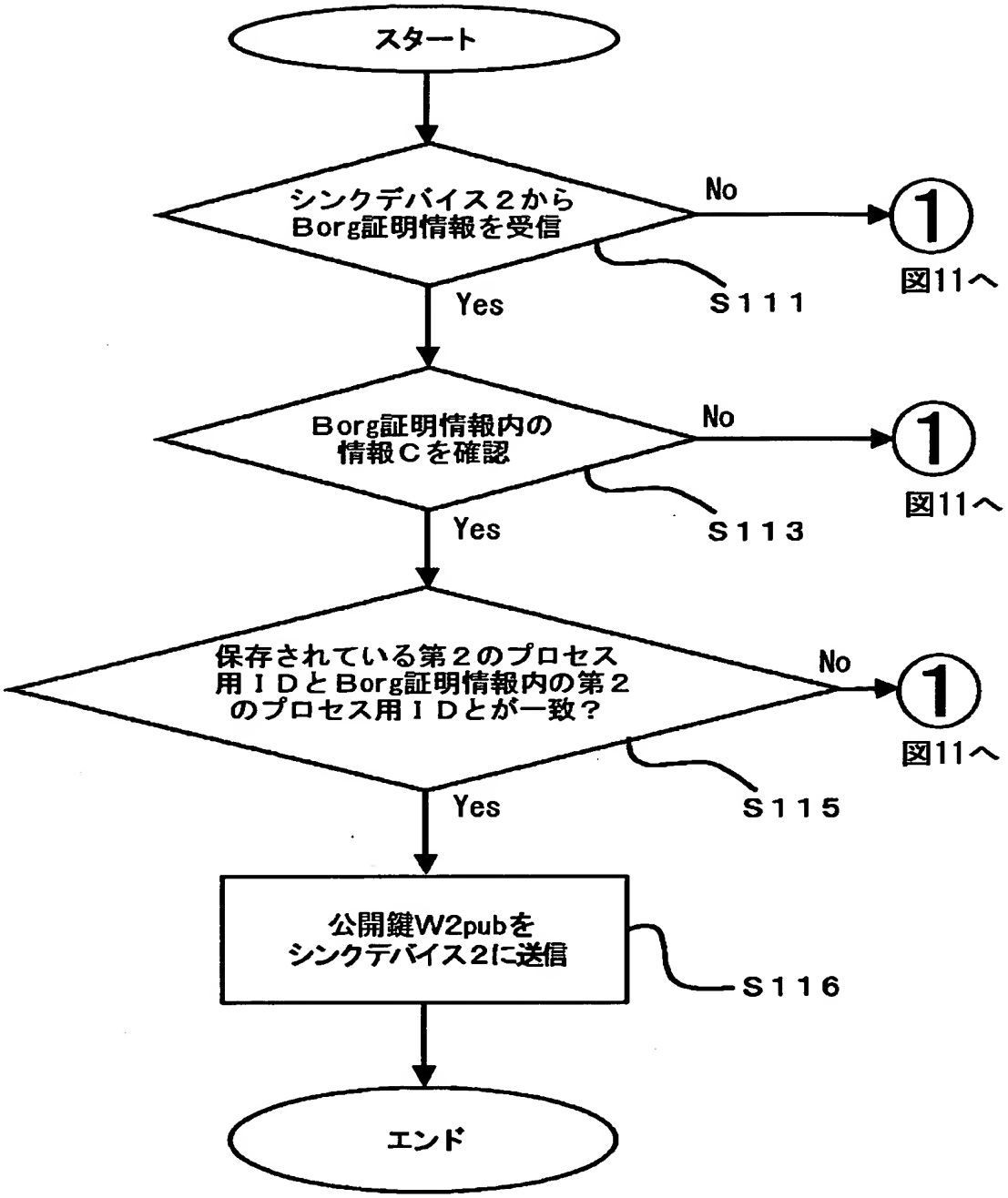
【図１】


スタート
シンクデバイス２から
情報Ｂを受信
No
Yes
Ｓ１０１
公開鍵Ｙpubを確認
No
①
図11へ
Yes
Ｓ１０３
第２のプロセス用ＩＤを
確認
No
①
図11へ
Yes
Ｓ１０５
第２のプロセス用ＩＤをメモリ７に
記録
Ｓ１０７
シンクデバイス２に
認証の成功を通知
Ｓ１０９
エンド

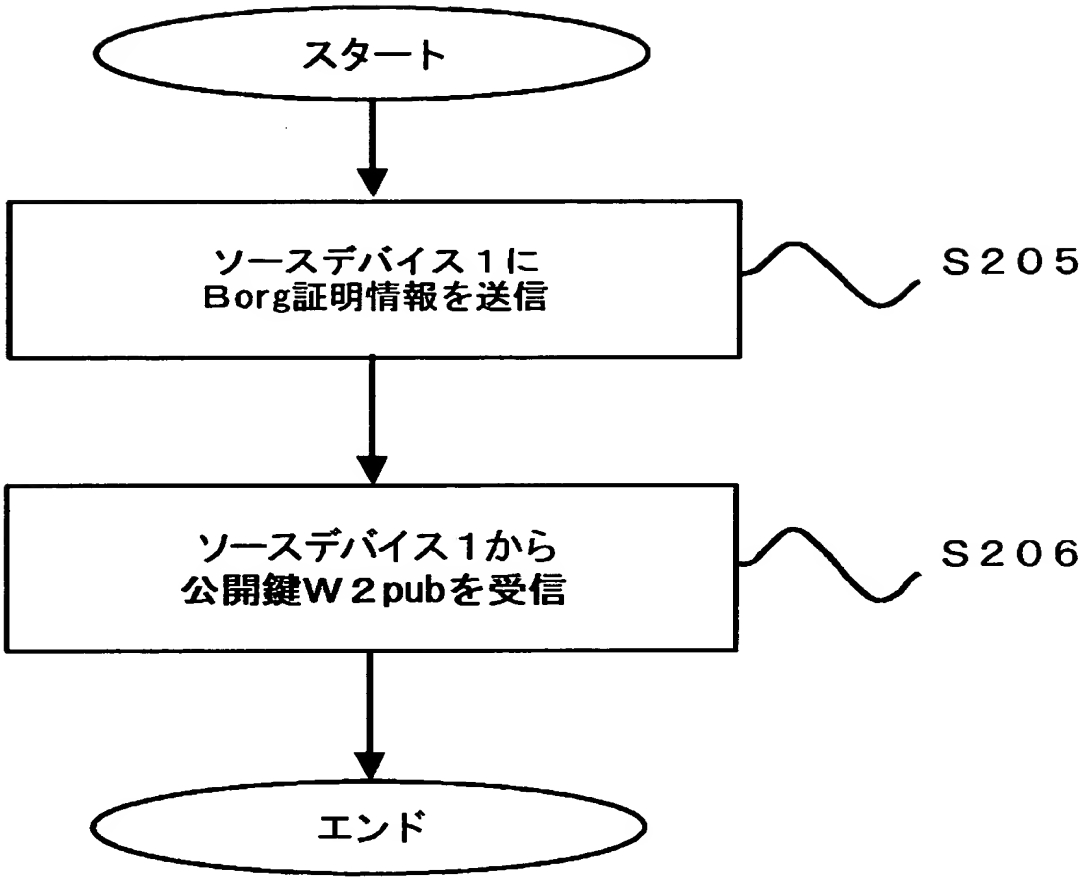
【図２】


スタート
ソースデバイス１に情報Ｂを送信
Ｓ２０１
ソースデバイス１から認証の
成功の通知を受信
No
Yes
Ｓ２０３
エンド

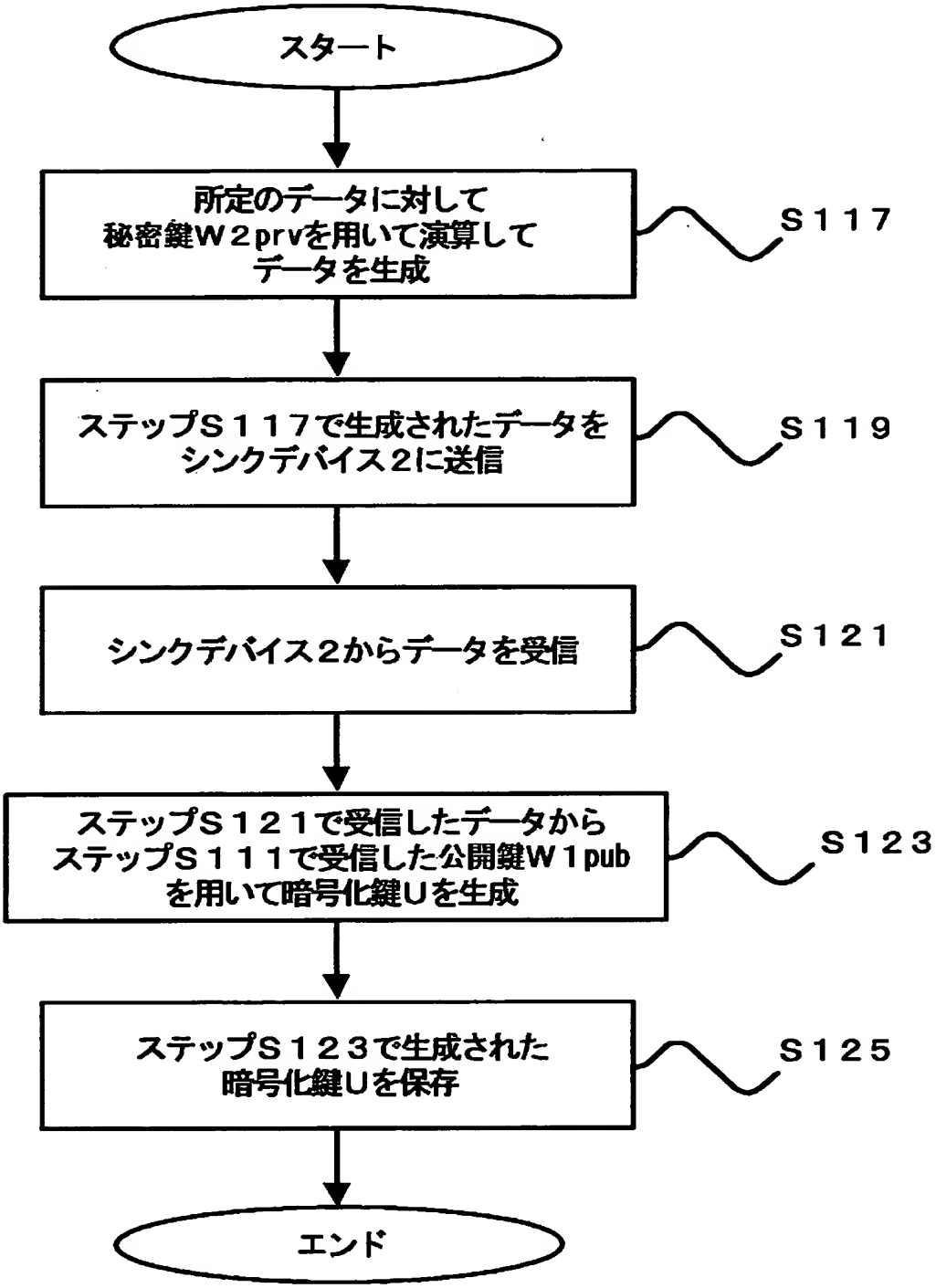
【図３】


スタート
シンクデバイス２から
Borg証明情報を受信
No
①
図11へ
S１１１
Yes
Borg証明情報内の
情報Ｃを確認
No
①
図11へ
S１１３
Yes
保存されている第２のプロセス
用ＩＤとBorg証明情報内の第２
のプロセス用ＩＤとが一致？
No
①
図11へ
S１１５
Yes
公開鍵W2pubを
シンクデバイス2に送信
S１１６
エンド

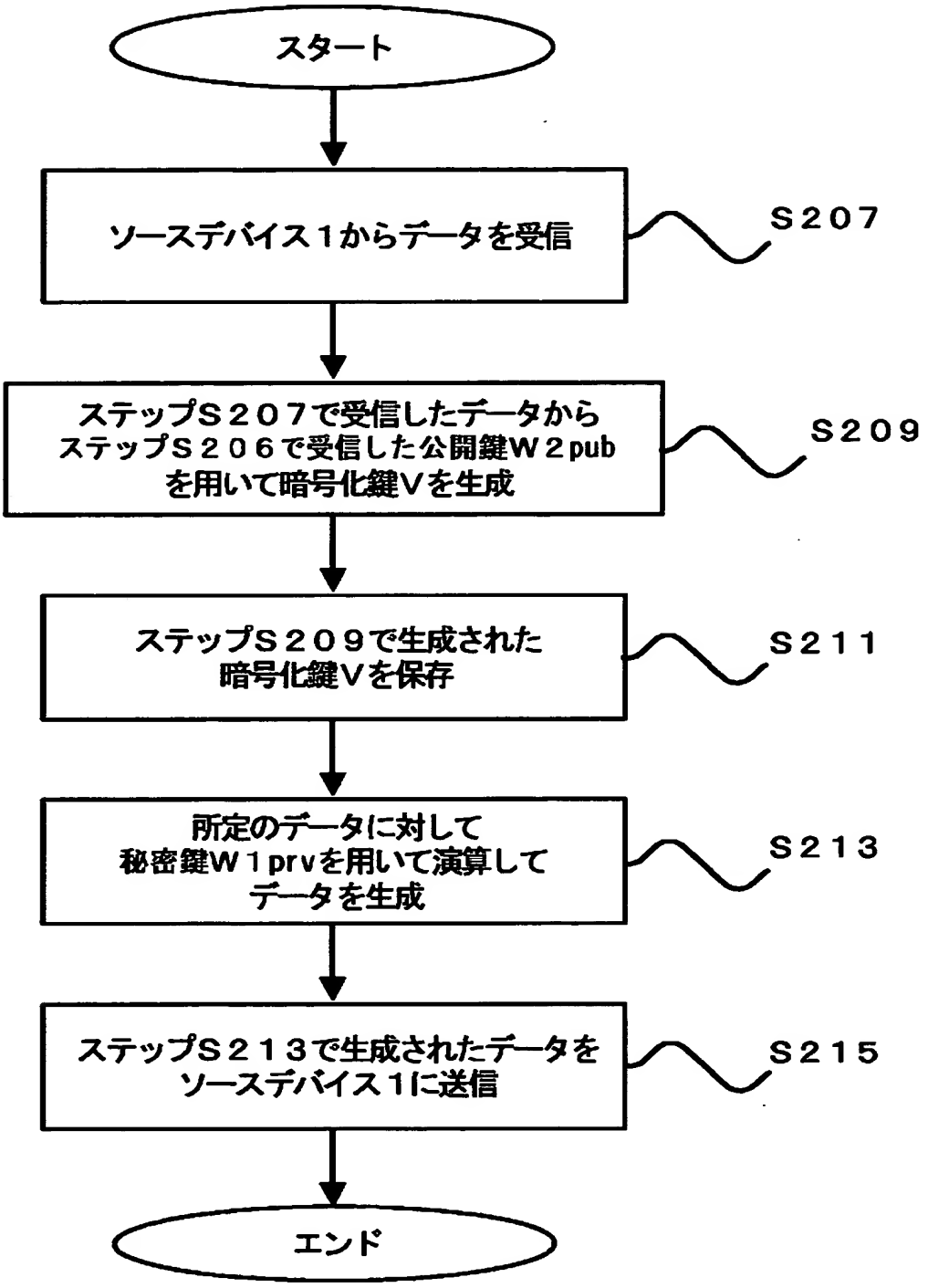
【図４】


スタート
ソースデバイス１に
Borg証明情報を送信
S２０５
ソースデバイス１から
公開鍵W２pubを受信
S２０６
エンド

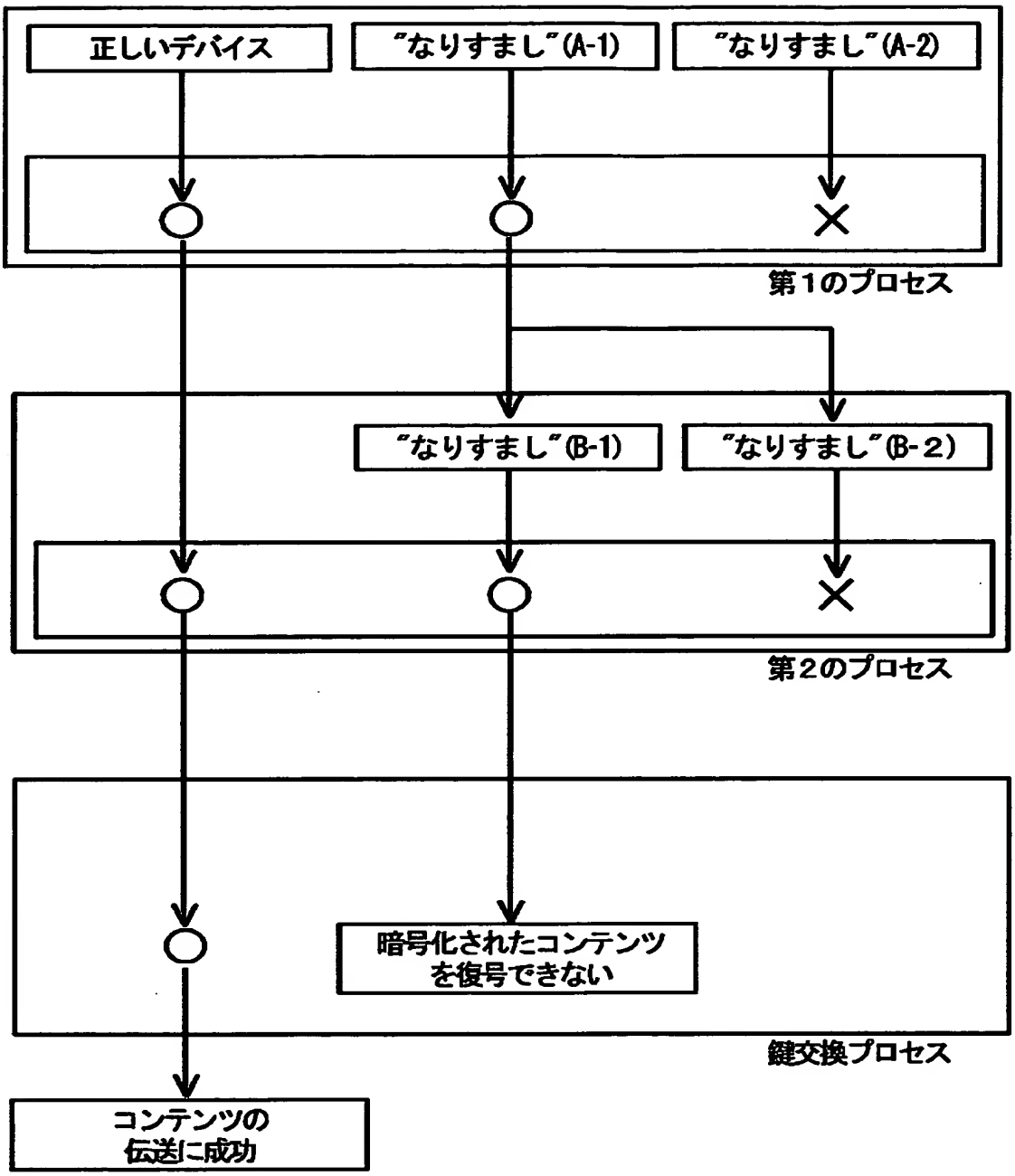
【図５】


スタート
所定のデータに対して
秘密鍵Ｗ２prvを用いて演算して
データを生成
Ｓ１１７
ステップＳ１１７で生成されたデータを
シンクデバイス２に送信
Ｓ１１９
シンクデバイス２からデータを受信
Ｓ１２１
ステップＳ１２１で受信したデータから
ステップＳ１１１で受信した公開鍵Ｗ１pub
を用いて暗号化鍵Ｕを生成
Ｓ１２３
ステップＳ１２３で生成された
暗号化鍵Ｕを保存
Ｓ１２５
エンド

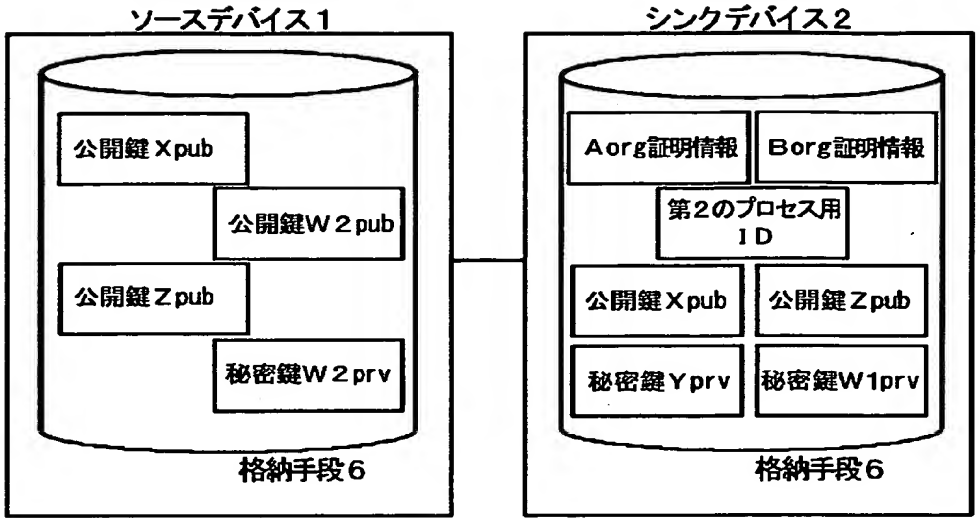
【図６】


スタート
ソースデバイス１からデータを受信
S207
ステップＳ２０７で受信したデータから
ステップＳ２０６で受信した公開鍵Ｗ２pub
を用いて暗号化鍵Ｖを生成
S209
ステップＳ２０９で生成された
暗号化鍵Ｖを保存
S211
所定のデータに対して
秘密鍵Ｗ１prvを用いて演算して
データを生成
S213
ステップＳ２１３で生成されたデータを
ソースデバイス１に送信
S215
エンド

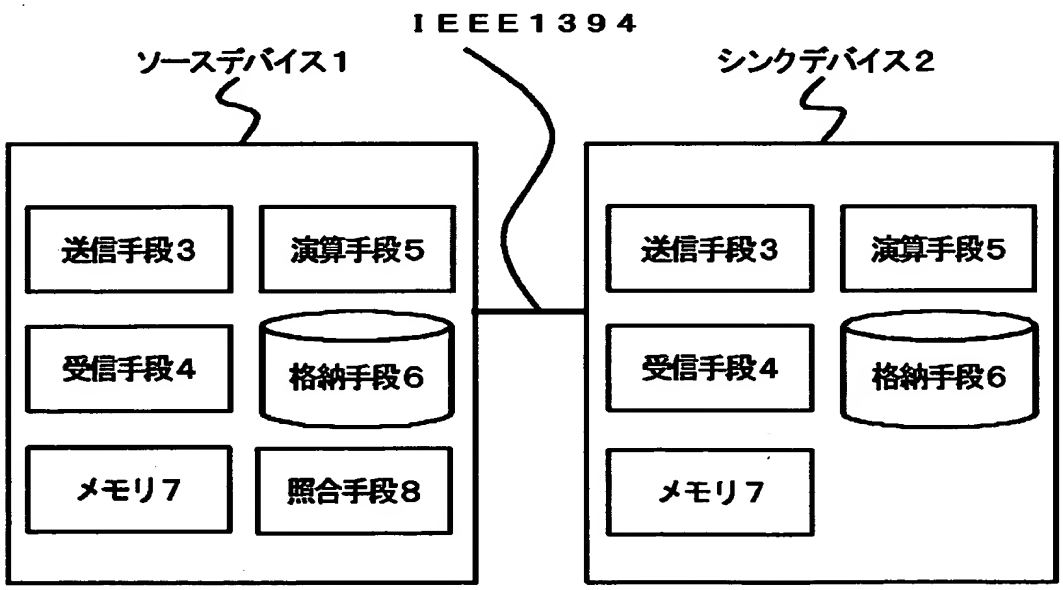
【図７】


正しいデバイス
"なりすまし"(A-1)
"なりすまし"(A-2)
第1のプロセス
"なりすまし"(B-1)
"なりすまし"(B-2)
第2のプロセス
暗号化されたコンテンツ
を復号できない
鍵交換プロセス
コンテンツの
伝送に成功

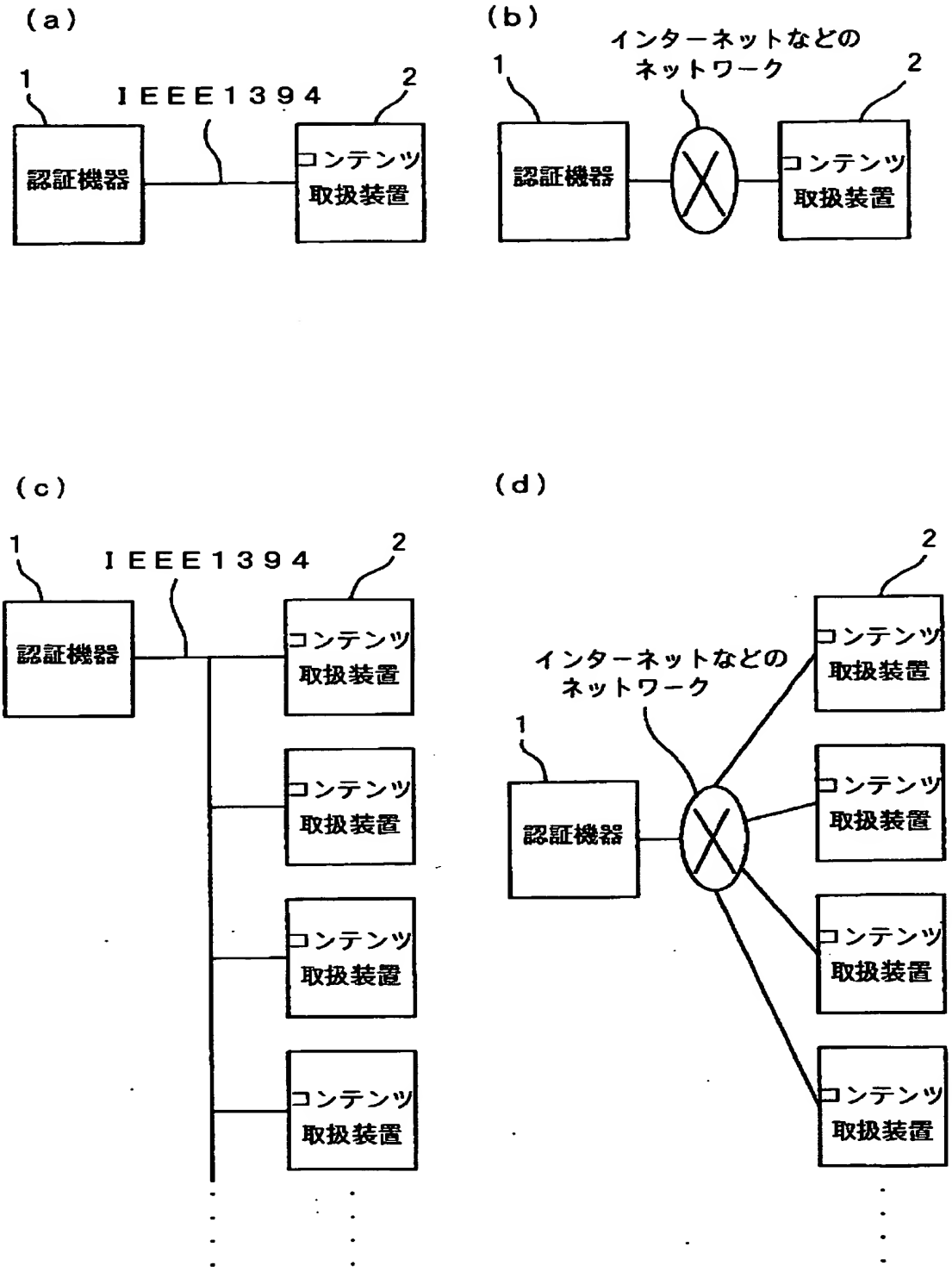
【図８】


ソースデバイス１
公開鍵Ｘpub
公開鍵Ｗ２pub
公開鍵Ｚpub
秘密鍵Ｗ２prv
格納手段６
シンクデバイス２
Aorg証明情報
Borg証明情報
第２のプロセス用ＩＤ
公開鍵Ｘpub
公開鍵Ｚpub
秘密鍵Ｙprv
秘密鍵Ｗ1prv
格納手段６

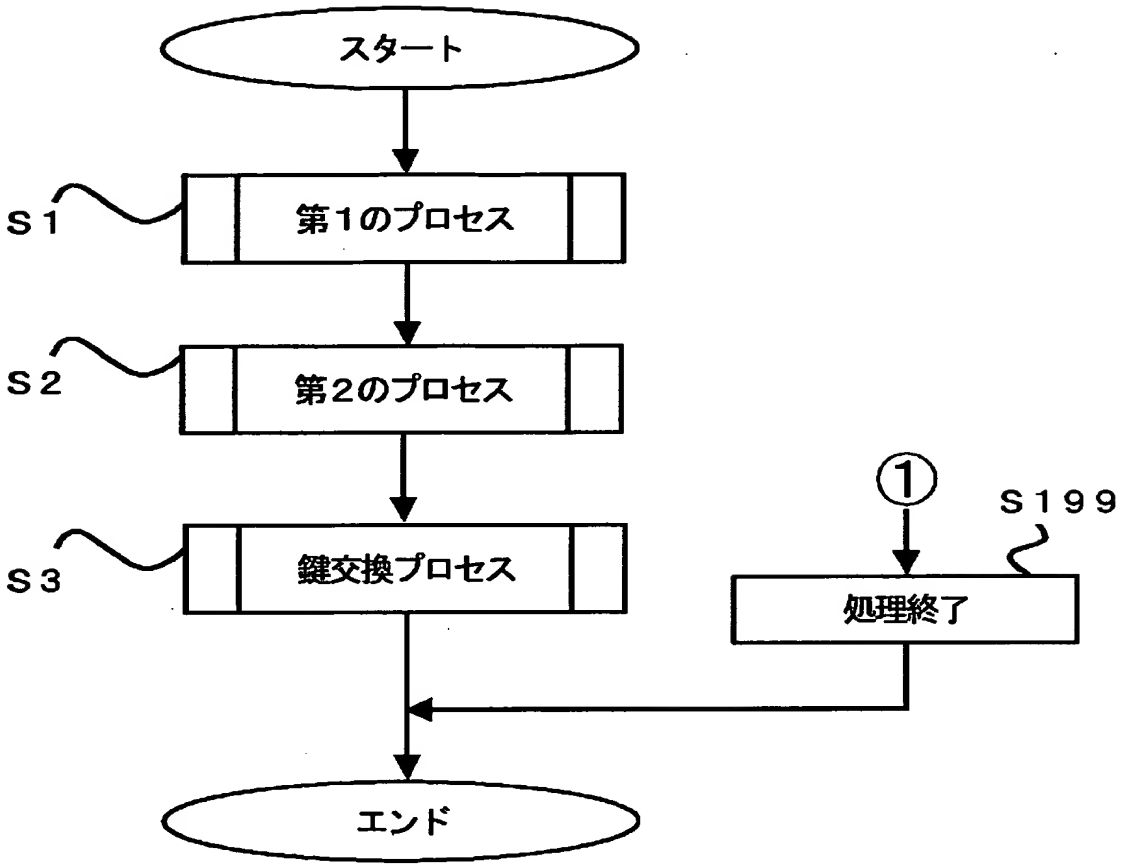
【図９】


ＩＥＥＥ１３９４
ソースデバイス１
シンクデバイス２
送信手段３
演算手段５
受信手段４
格納手段６
メモリ７
照合手段８
送信手段３
演算手段５
受信手段４
格納手段６
メモリ７

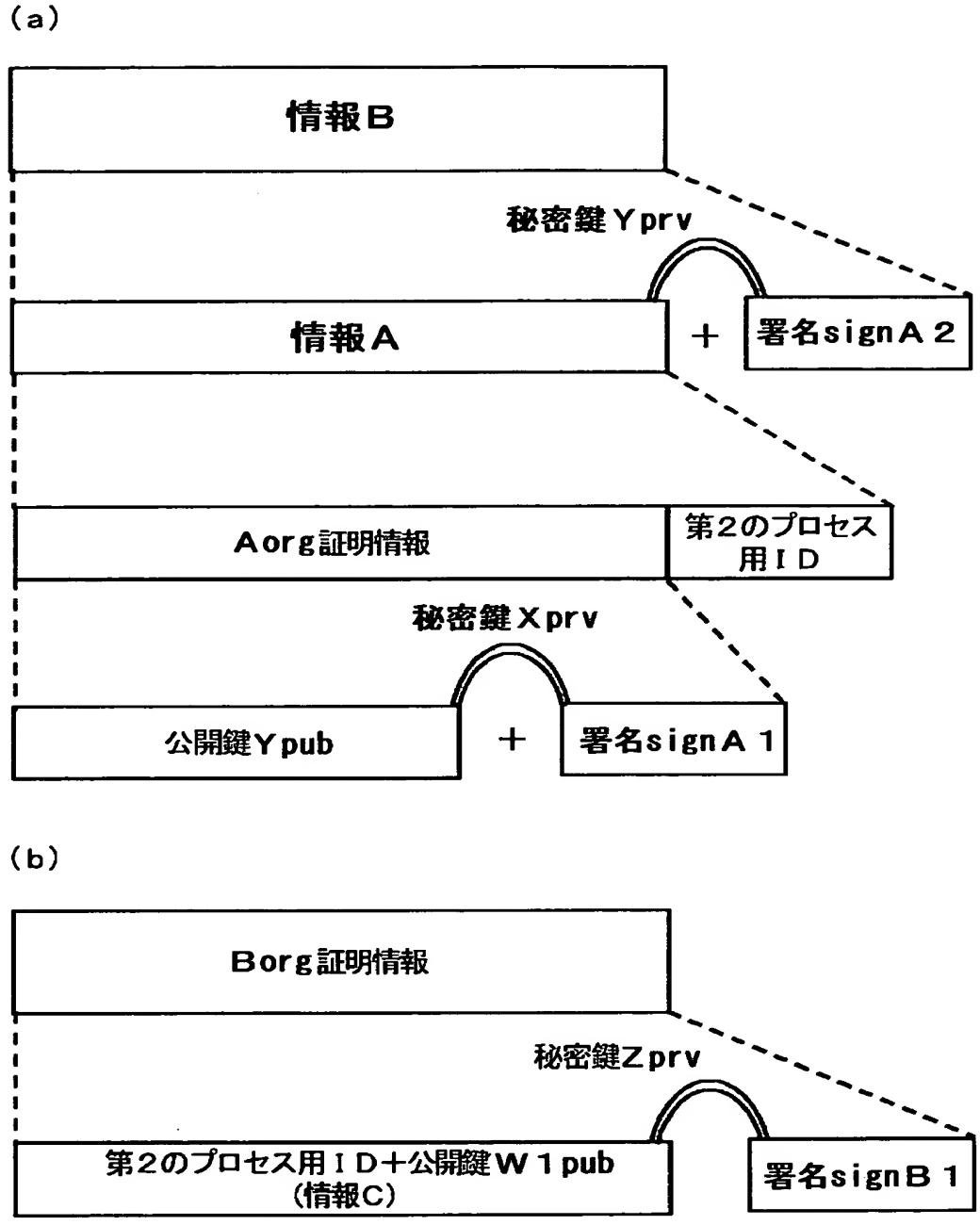
【図１０】


(a)
1
IEEE1394
2
認証機器
コンテンツ
取扱装置
(b)
インターネットなどの
ネットワーク
1
2
認証機器
コンテンツ
取扱装置
(c)
1
IEEE1394
2
認証機器
コンテンツ
取扱装置
コンテンツ
取扱装置
コンテンツ
取扱装置
コンテンツ
取扱装置
(d)
2
インターネットなどの
ネットワーク
1
認証機器
コンテンツ
取扱装置
コンテンツ
取扱装置
コンテンツ
取扱装置
コンテンツ
取扱装置

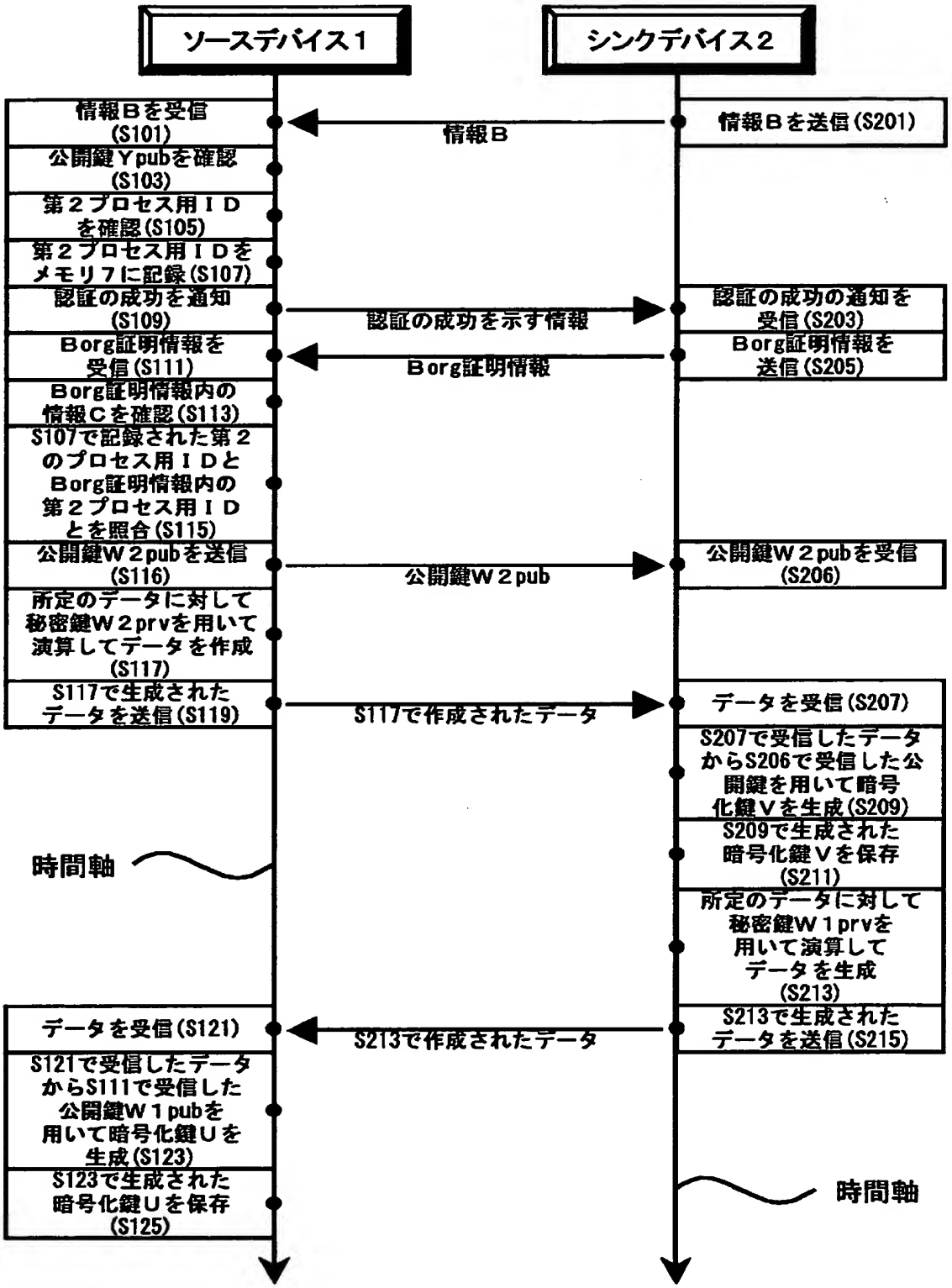
【図１１】



【図１２】


(a)
情報B
秘密鍵Yprv
情報A
＋
署名signA２
Aorg証明情報
第2のプロセス用ＩＤ
秘密鍵Xprv
公開鍵Ypub
＋
署名signA１
(b)
Borg証明情報
秘密鍵Zprv
第2のプロセス用ＩＤ+公開鍵Ｗ１pub
(情報C)
署名signＢ１

【図１３】


ソースデバイス１
シンクデバイス２
情報Ｂを受信(S101)
情報Ｂ
情報Ｂを送信(S201)
公開鍵Ｙpubを確認(S103)
第２プロセス用ＩＤを確認(S105)
第２プロセス用ＩＤをメモリ７に記録(S107)
認証の成功を通知(S109)
認証の成功を示す情報
認証の成功の通知を受信(S203)
Ｂorg証明情報を受信(S111)
Ｂorg証明情報
Ｂorg証明情報を送信(S205)
Ｂorg証明情報内の情報Ｃを確認(S113)
S107で記録された第２のプロセス用ＩＤとＢorg証明情報内の第２プロセス用ＩＤとを照合(S115)
公開鍵Ｗ２pubを送信(S116)
公開鍵Ｗ２pub
公開鍵Ｗ２pubを受信(S206)
所定のデータに対して秘密鍵Ｗ２prvを用いて演算してデータを作成(S117)
S117で生成されたデータを送信(S119)
S117で作成されたデータ
データを受信(S207)
S207で受信したデータからS206で受信した公開鍵を用いて暗号化鍵Ｖを生成(S209)
S209で生成された暗号化鍵Ｖを保存(S211)
所定のデータに対して秘密鍵Ｗ１prvを用いて演算してデータを生成(S213)
データを受信(S121)
S213で作成されたデータ
S213で生成されたデータを送信(S215)
S121で受信したデータからS111で受信した公開鍵Ｗ１pubを用いて暗号化鍵Ｕを生成(S123)
S123で生成された暗号化鍵Ｕを保存(S125)
時間軸
時間軸

【書類名】　　要約書

【要約】

【課題】　ソースデバイス（コンテンツ送信側機器）からシンクデバイス（コンテンツ受信側機器）にコンテンツを送信する際、コンテンツを盗取されずに所望のシンクデバイスに確実に送信可能となるよう認証を行う。

【解決手段】　第１の管理機関からライセンスを受けている証明となるシンクデバイス２の証明情報と第２の管理機関により管理されているシンクデバイス２の識別情報とが結合されたものに署名が付加された情報をシンクデバイス２からソースデバイス１に送信し、ソースデバイス１でその証明情報を認証し、さらにその証明情報を参照して署名を認証して、シンクデバイス２の識別情報を記録手段に記録する。続いて、再びシンクデバイス２の識別情報をシンクデバイス２からソースデバイス１に送信し、この情報を受信したソースデバイス１で、この情報と記録手段に記録されたシンクデバイス２の識別情報とを照合する。

【選択図】　　図９

認定・付加情報

特許出願の番号	特願２０００－１３３９５７
受付番号	５００００５６０５５７
書類名	特許願
担当官	第七担当上席　００９６
作成日	平成１２年　５月　８日

＜認定情報・付加情報＞

【提出日】　平成12年 5月 2日

次頁無

出　願　人　履　歴　情　報

識別番号　　〔０００００４３２９〕

１．変更年月日　　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社